Challenges of Cybersecurity Research in a Multi-user Cyber-Physical Testbed

Thomas Edgar
Pacific Northwest National Laboratory
Richand, Washington 99354
Email: thomas.edgar@pnnl.gov

Tom Carroll
Pacific Northwest National Laboratory
Richand, Washington 99354
Email: thomas.carroll@pnnl.gov

David Manz
Pacific Northwest National Laboratory
Richand, Washington 99354
Email: david@pnnl.gov

I. Introduction

Deployed Cyber-Physical Systems (CPSs)[5] are often large, complex, and expensive environments that utilize specialized equipment. The equipment is difficult to configure, deploy, and maintain and requires much expertise to correctly instantiate the components into a connected, functional system [3]. The number of individuals with the necessary skill sets is small, and they are expensive due to the high demand. These combined factors have traditionally limited researchers' access and their ability to conduct studies. A multi-user remotely-accessible testbed[6] significantly lowers the barrier of entry by providing researchers with ready access to CPS environments, without them individually needing to invest in the equipment, resources, and expertise to deploy them. Most importantly, users are freed to focus on research and not ancillary system duties.

A multi-user testbed is a shared resource whose equipment acquisitions benefit all users. CPSs are in essence a "system of systems;" a diverse, broad range of equipment is required to research the many faucets of CPSs. Equipment diversity enables modeling realistic environments in multiple domains. Multi-vendor equipment supports interoperability studies and vulnerability assessments. Finally, equipment diversity assists investigators in generalizing results.

Robust scientific experimentation demands repeatable results [4]. When conducted on a testbed, the description of the *system under test* is the testbed configuration and normally includes the equipment, initial configuration, the relationship between devices, and the communication links. Another researcher can then independently verify the results on the testbed.

A multi-user CPS testbed provides significant benefits to cybersecurity research. However, there are notable challenges to creating such a testbed. These challenges are assessed in this paper. The next section summarizes the challenges. The following section discusses avenues for solving these challenges in the context of the power networking, equipment, and technology (powerNET) testbed. Finally, a conclusion section discusses a path forward for the future.

II. Challenges for Cyber-Physical security research using testbeds

The unique characteristics of cyber-physical systems and a multi-user experimental testbed result in unique challenges for cybersecurity experimentation. Cyber-physical systems have similar issues to general enterprise cybersecurity experimentation such as data sensitivities, experimental separation, and testbed fidelity but cyber-physical systems have additional unique issues. For example, cyber-physical systems add challenges like system scale, physical process simulation, and diversity design. The cybersecurity challenges that have been encountered during the process of designing and implementing a multi-user experimental cyber-physical testbed will be discussed in this section.

Operational IT systems often have data security requirements that require protection. This encompasses Personally Identifiable Information (PII) and Intellectual Property (IP). Cyber-physical systems can also include these issues, but also add problems such as the proprietary nature of the module or architecture of the system and the operational state of their systems. For example, the state estimation models used by control room operators of the electrical grid as well as the data that provides a status of the system can be proprietary. These models and data could provide competitors or threat actors with system weaknesses that could be leveraged for financial gain or exploitation. Due to the data security requirement, a multi-user experimental cyber-physical testbed has the challenge of providing adequate security mechanisms to ensure that only the appropriate users can access data as well as no data leakage of how an experiment may be architected.

Data is not the only protection challenge that must be addressed in a multi-user experimental testbed. Resources must be protected to ensure that one experiment does not impact the results of another. Multiple experiments could be running on the testbed at any time. The effects of one must not impact the others or at a minimum, quantification of the effects of the testbed on an experiment need to be documented for the other experimenters. This must be a part of every testbed used and is necessary for rigorous experimental design. For example, if one experiment is testing the effects of a DoS attack on a system and another experiment is performing a vulnerability assessment of a product it would be incorrect if the second experimenter believed a loss of connectivity to a device was significant to their actions when in reality it was due to the DoS experiment impacting the shared networking resources [2]. Since cybersecurity experimentation often tests abnormal operational cases it is a challenge to protect experiments from impacting others. Also, it is a challenge to quantify impacts when they do occur. This last step is crucial for all assumptions and qualifications made in a testbed.

Cyber-physical systems run the gamut of scale; from small self-contained systems like automobiles up to highly complex systems-of-systems like electrical grids. Providing the capability to scale a testbed to meet the needs of a broad range of applications is a challenge. The equipment involved in cyber-physical systems are often expensive to buy and configure. The equipment is often hardened for harsh environmental conditions and requires compliance with many safety and reliability standards. Also, the expertise needed to configure and maintain these systems is highly specialized and expensive to acquire.

On top of the scalability challenge is the heterogeneous nature across and within cyber-physical industries. Systems designed for cyber-physical systems are derived from the requirements of the physical processes for which they are monitoring and/or controlling. Therefore, a system in the manufacturing industry is significantly different than one in the transportation industry. This can include different equipment, network architecture, and operational performance and security requirements. However, this challenge goes deeper, and there can be extensive differences even within industries. For example, due to geography constraints an electric utility in a plains state can look significantly different than one that operates over mountainous terrain.

Another issue that can occur due to scaling of experiments is fidelity of the system. Depending on the experimental design, simulated equipment may not reach the fidelity requirements to evaluate the security characteristics of a device. On the other end, an experiment to evaluate the impact of an event on the electrical grid does not require the fidelity of having the actual equipment for the grid. Ensuring a multi-user experimental testbed has the ability to meet the fidelity needs of a broad range of experimentation is a challenge.

Integration of the physical process into the testbed is a closely related challenge intertwined with fidelity. CPS requires a data substrate which is the physical processes they monitor and control. This substrate interplays with the CPS, providing input and reacting to output. It is often difficult if not impossible to replicate these physical processes in a laboratory environment. Therefore, a simulation capability is necessary to provide the physical aspect of CPS. Creating a simulation capability with high enough fidelity to model the real world is challenging.

III. powerNET: Driving Solutions Forward

The power networking, equipment, and technology (powerNET) testbed [1] is an implementation of a multi-user experimental CPS testbed. In this section, powerNET will be introduced and the envisioned path to solve the challenges defined in the previous section. PowerNET is an effort to build a testbed capability that is multi-user, remotely and dynamically configurable, and user friendly.

In order to provide the necessary data and network separation between users and experiments, powerNET uses a variety of technologies. Each user and project are provided with networked shared directories via NFSv4. To provide authentication and authorization services, Kerberos is utilized. Scripts built into the testbed OS images, on startup, retrieve user and project keys to mount the shares and provide access. Virtual LANs are utilized to provide separation between experiment network traffic. Additionally, overprovisioning of shared resources will alleviate cross experimental impacts.

powerNET provides a unique capability to provide scalability and different levels of fidelity. powerNET combines simulation, virtualization, emulation, and real cyber-physical equipment in one testbed. This combination enables high fidelity small scale experimentation with bare metal equipment. However, it can also scale up to medium scale and slightly less fidelity with virtualization and emulation. Lastly, simulations can be run to enable experimentation at large scales. The combination of all three enable a flexible environment that can change based on the needs of the experimenters.

Similarly, powerNET was designed modularly and for dynamic configuration to enable a broad spectrum of research. CPS includes a diverse selection of industries and equipment. While powerNet currently has a focus on a subset of power transmission and distribution applications, its modular design enables expansion into other applications within the power industry and even into other cyber-physical domains (i.e. oil/ natural gas, water/ waste water, transportation, etc). And due to the heterogeneous architecture of the industries, powerNET is dynamically configurable so as to enable the modeling of a wide range of realistic architectures.

There are multiple avenues to integrate simulation of physical processes into a multi-user testbed. The simplest but least accurate option is to perform complete simulation of the process and equipment. With a higher fidelity, process simulators can be leveraged to generate data files that represent the instrumentation of the physical world. These data files can then be used to generate digital and analog I/O that can be fed into the CPS equipment. However, this method does not create a reactive experiment. The highest fidelity would be to dynamically integrate physical processes into a testbed. This can be done be via a real-time running simulator that can inject digital and analog I/O while also be able to respond to communication from the CPS equipment. The Real Time Digital Simulator, used in the power industry, is an example of such a capability. All three have their uses and are viable options depending on the experimental setup. During experimental design, researchers must be aware of the level of fidelity offered by testbeds with differing configurations and choose the appropriate setup based on experimental requirements. This needs to be an explicit part of experimental setup and design and not an implicit, or perhaps overlooked afterthought.

IV. Conclusion

While a multi-user (CPS) testbed has many benefits, some operational challenges must be addressed. The set of challenges defined in this paper are by no means a complete enumeration. The challenges listed are the most pressing that have been analyzed in the development of the powerNET testbed. Some of the challenges discussed are significant and may require research efforts of their own.

In addition to these challenges, there exists a more fundamental generalization issue or external validity problem for all of cybersecurity science. The field still lacks good protocol to quantify how well the demonstration of a security solution in one context would apply to the broader community. Also, the cyber domain is quickly evolving and cybersecurity science still lacks a method to apply research results into predictive quantification of how a solution will stand up to threat evolution.

The powerNET approaches discussed in this paper provide a good starting point in tackling the challenges listed. However, in most cases they do not provide a complete solution to the challenge. It is necessary that further work is performed to enable the full capabilities that are desirable in a multi-user CPS testbed.

Acknowledgment

This research is funded by US Department of Energy and US Department of Homeland Security under contract DE-AC05-76R1-1830. powerNET is a part of the Pacific Northwest National Laboratory Future Power Grid Initiative GridOptics capabilities.

References

[1] TW. Edgar, DO. Manz AD. McKinnion, TW. Carroll, BA. Akyol, PM. Skare, CW. Tews, and JC. Fuller, *Power Networking, Equipment, and Technology Experimentation: Designing a Testbed for Cyber-Physical Security Research*, In 7th Annual Cyber Security and Information Intelligence Research Workshop. Association for Computing Machinery, New York, NY, 2012.

[2] Roman Chertov and Sonia Fahmy and Ness B. Shroff, ACM Trans. Model. Comput. Simul., *Fidelity of Network Simulation and Emulation: A Case Study of TCP-Targeted Denial of Service Attacks*, Num.1, Vol. 19, 2008.

[3] E. A. Lee, *Cyber physical systems: Design challenges*, Eletrical Engineering and Computer Sciences, University of California at Berkley, Tech. Rep. UCB/EECS-2008-8, Jan. 23, 2008, accessed on Apr. 22, 2011

[4] E. Eide, *Toward replayable research in networking and systems*, in Proc. of the NSF Workshop on Archiving Experiments to Raise Scientific Standards (Archive 10), 2010.

[5] National Science Foundation, *Cyber-physical systems program solicitation*, 2011, accessed on Apr. 25, 2011.

[6] J. Kurose et al., *Report of NSF Workshop on Network Research Testbeds*, Nov. 2002.